

EXHIBIT A

1 of 3 DOCUMENTS

Copyright 2007 States News Service
States News Service

April 25, 2007 Wednesday

LENGTH: 351 words

HEADLINE: STEVENS ID THEFT PREVENTION ACT PASSES COMMERCE COMMITTEE

BYLINE: States News Service

DATELINE: WASHINGTON

BODY:

The following information was released by Senate Committee on Commerce, Science and Transportation:

The Senate Committee on Commerce, Science and Transportation today passed S. 1178 the "Identity Theft Prevention Act." Committee Vice Chairman Senator Ted Stevens (R-Alaska) introduced the legislation and it is cosponsored by Commerce Committee Chairman Daniel Inouye (D-Hawaii), Senator Gordon Smith (R-Ore.) and Senator Mark Pryor (D-Ark.) and Senator Bill Nelson (D-FL). This bill would strengthen information safeguards and ensure notification to consumers whose sensitive personal information has been acquired without authorization. The bill would also direct the Federal Trade Commission (FTC) to enforce rules to protect such information. Under the bill, consumers would be able to freeze their credit for a reasonable fee to protect themselves from identity theft. The bill now moves to the Senate where it awaits consideration.

"ID theft is a growing problem that plagues Americans in the far reaches of our nation and everywhere in between," said Senator Stevens. "Studies of identity theft show that Alaskans are particularly susceptible to this criminal activity. It is time for Congress to act. We must take steps to help people protect themselves. I urge the Senate to take up this bill, which has received broad bipartisan support, and pass it quickly."

Identity theft has risen dramatically nationwide over the past decade and the FTC estimates that each year nearly 9 million Americans - or roughly 4.6 percent of the domestic adult population - are victimized by identity thieves. The FTC indicates that physical and online identity theft accounted for 40 percent of the more than 616,000 consumer fraud complaints filed last year with the agency. The costs associated with identity theft are enormous. In 2006, it is estimated that the losses to businesses and financial institutions due to identity theft totaled \$52.6 billion, and the out-of-pocket losses to consumers totaled \$5 billion, which does not take into account the average 300 hours spent by each victim to restore their good name.

LOAD-DATE: April 26, 2007

EXHIBIT B

1 of 1 DOCUMENT

Copyright 2005 Factiva, a Dow Jones and Reuters Company
All Rights Reserved



(Copyright (c) 2005, Dow Jones & Company, Inc.)

THE WALL STREET JOURNAL.

The Wall Street Journal

October 8, 2005 Saturday

SECTION: Pg. B1

LENGTH: 1438 words

HEADLINE: Identity Theft -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way

BYLINE: By Robin Sidel

BODY:

WORRIED THAT shadowy gangs of Russian hackers are breaking into computer networks, stealing your financial secrets? Don't lose too much sleep over it.

But you might want to hide your checkbook when friends and relatives come visit your home.

Despite a series of alarming reports in recent months about security breaches that have made personal data potentially vulnerable to crooks -- such as the one at credit-card processor CardSystems Solutions Inc. affecting 40 million credit-card accounts -- most bank-related crimes remain stubbornly low-tech. They range from simple forgery of a check, to unauthorized credit-card use, to Dumpster-diving, which is when someone plucks a bank statement or credit-card bill from your garbage.

And the perpetrator probably may not be a stranger.

According to one recent study, by Javelin Strategy & Research, a consulting firm in Pleasanton, Calif., in 26% of all cases the fraud victims knew the person who had misused their personal information. (Typically it was a family member, friend or neighbor, or in-home employee.) In addition, as much as 50% of debit-card fraud occurs when a card is snagged by a family member or friend who knows the card's personal-identification number, according to a recent report from TowerGroup, a unit of MasterCard International Inc.

The term "identity theft" is often used loosely to describe a wide array of crimes. But true identity theft occurs when someone uses stolen information to create a new form of identity, such as opening a new credit-card account under the victim's name. That differs significantly from other kinds of bank fraud, such as when a criminal uses a stolen ATM card to get cash out of a teller machine.

Identity Theft -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way
The Wall Street Journal October 8, 2005 Saturday

Whether it's full-blown ID theft or small-scale fraud, even in cases where the criminal is a stranger, it's almost never a case of sophisticated computer hacking. Although 75% of all households use the Internet and 65% of those do some online banking, "most criminals obtain personal information through traditional rather than electronic channels," according to the Javelin study. Some 29% of victims surveyed said their personal information was obtained through a lost or stolen wallet, checkbook or credit card.

According to the study, the bulk of the rest were attributed to friends and relatives, corrupt employees, stolen mail, Dumpster-diving, and computer spyware. Computer viruses or hackers accounted for only 2.2% of incidents. While there has been a significant increase in the number of electronic attempts at identity theft, "the ones that are working are the traditional ones," said James Van Dyke, Javelin's president.

The Federal Trade Commission itself defines identity theft broadly, describing it as when someone possesses or uses a person's personal or financial information without their knowledge with the intent of committing fraud or other crimes.

The commission estimates that identity theft affects nearly 5% of the adult population, costing businesses and individuals a combined \$53 billion annually. It received 246,000 reports of identity theft last year, nearly triple the number received in 2001. The FTC has attributed much of that rise to heightened awareness of the issue among consumers, making them more likely to report incidents as identity theft.

Overall, statistics on identity theft are spotty. For one thing, research has found that most victims of identity theft don't report the crime to police. In many cases, they aren't even certain that they are truly crime victims and don't know how the incident occurred. Banks increasingly alert authorities when incidents occur, but even those disclosures can be incomplete.

There are a number of steps individuals can take to protect themselves.

Many financial institutions are increasingly urging their clients to start using paper shredders at home. Household models can be relatively inexpensive, and they significantly reduce the chances that a criminal can find any useful personal information in the trash. Banks typically recommend shredding documents that contain account information, Social Security numbers, credit-card and ATM receipts and credit-card offers. Also, shred blank checks that sometimes come in the mail as part of a solicitation.

Another suggestion: Be particularly aware if credit-card bills or bank statements are missing from the mailbox. If a bill arrives more than two weeks late, the American Bankers Association suggests contacting the local post office to be sure it isn't being forwarded without the recipient's knowledge. Also check with the company where the bill originated.

It's also wise to avoid disclosing any personal information on forms or applications unless absolutely necessary, says Mike Cunningham, senior vice president in the credit-card fraud department at J.P. Morgan Chase & Co.

As an example, Mr. Cunningham says, he was recently filling out an application to be a coach on his son's neighborhood football team in Arizona, and the form asked for his social security number, driver's license number and other personal information. He declined to provide the information, because there was no way for him to know whether his personal information would be kept under lock and key.

"I just told the team mom that I didn't see why they needed it -- it was the perfect amount of information for an identity thief," he said. He got the job anyway.

The only organizations you're required to provide with your social security number are your employer and your financial institutions. (This is for tax purposes.) If anyone else asks -- say, a retailer -- you don't have to give it. The company can decline to provide the service, but it's worth asking what other identification they might accept instead.

Identity Theft -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way
The Wall Street Journal October 8, 2005 Saturday

Amid the proliferation of old-fashioned fraud, some financial institutions are fighting back by urging their customers to abandon paper statements altogether and instead view their accounts online. Among them is E*Trade Financial Corp., which says its online system is more secure than paper statements that can be stolen or copied. A spokeswoman declined to specify how much money the company will save by eliminating the printing and mailing of paper statements.

Banks are having a particularly tough time battling one of the oldest and most common kinds of crime: check fraud. Attempts of check fraud rose to \$5.5 billion in 2003 from \$4.3 billion in 2001, according to the American Bankers Association. The incidents resulted in losses of \$677 million, representing a slight decline from \$698 million in 2001; the trade group attributed the drop to better fraud-detection methods.

That slight decline isn't so reassuring to Lee Roberts, senior vice president at National Penn Bancshares Inc., a regional bank based in Boyertown, Pa. As recently as the past few weeks, the bank has been hit by a wave of incidents in which criminals have copied checks and then altered them for fraudulent use. That practice "has been around for seven or eight years," says Mr. Roberts. But as photocopiers and image-manipulation computer software become more sophisticated, he says, "they're getting better at it."

Battling Identity Theft

Despite all the buzz about high-tech online identity theft, most instances revolve around old-fashioned fraud such as forging a signature on a check. Here are steps for reducing the risk:

-- Check up on yourself regularly

Get a copy of your credit report every year from each of the major credit bureaus (TransUnion, Equifax, Experian) to make sure the records are accurate. Also, closely review all monthly bank and billing statements for discrepancies.

-- Travel light

Avoid carrying around credit-card or personal documents unless you really need them.

-- Keep personal data under wraps

Don't share personal ID numbers or passwords with anyone. Don't provide information over the phone or hand over personal data unless you know why it is needed. Keep a list of all account numbers in a secure place so that you have quick access if cards or documents get stolen or lost.

-- Buy a shredder for the home

Tear up or shred all credit-card receipts and all new-card offers that arrive in mail. Also destroy all documents that contain account numbers or other personal financial information.

-- Check the mail

Don't let mail sit in the mailbox for days on end. And don't place sensitive outgoing mail, such as bills, in your home mailbox to await

Page 4

Identity Theft -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way
The Wall Street Journal October 8, 2005 Saturday

collection. Instead, drop it in a collection box.

Sources: Federal Trade Commission, American Bankers Association

NOTES:

PUBLISHER: Dow Jones & Company, Inc.

LOAD-DATE: October 8, 2005

EXHIBIT C

Page 17

Visa USA Announces Account Truncation Initiative to Protect Consumers from ID Theft; Visa CEO Announces New Initiative at Press Conference With Sen. Dianne Feinstein PR Newswire March 6, 2003 Thursday

6 of 9 DOCUMENTS

Copyright 2003 PR Newswire Association, Inc.
PR Newswire

March 6, 2003 Thursday

SECTION: WASHINGTON DATELINE

DISTRIBUTION: TO BUSINESS AND NATIONAL EDITORS

LENGTH: 774 words

HEADLINE: Visa USA Announces Account Truncation Initiative to Protect Consumers from ID Theft;
Visa CEO Announces New Initiative at Press Conference With Sen. Dianne Feinstein

DATELINE: WASHINGTON March 6

BODY:

At a press conference today on Capitol Hill with Senators Dianne Feinstein (D-CA), Judd Gregg (R-NH), Jon Corzine (D-NJ) and Patrick Leahy (D-VT), Visa USA CEO Carl Pascarella, announced Visa USA's new account truncation program to protect consumers from identity theft. The following are excerpts of Mr. Pascarella's remarks:

"I am here today to talk about the steps that Visa is taking to put identity theft protections in place. Visa USA and our Member financial institutions have a long history of using state of the art technology to further protect cardholder information. Visa was the first payments company to adopt a zero liability policy for unauthorized purchases, and we've continued this leadership role with Verified by Visa, which authenticates cardholders for Internet purchases, and our sophisticated neural networks that monitor spending anomalies.

"We have also implemented our Cardholder Information Security Program, or CISP, a set of 12 requirements for protecting cardholder data for which all Visa payment system participants need to comply. In fact, Visa is adding more resources to our auditing process to ensure any entity that touches a Visa transaction will be compliant with our Cardholder Information Security Program rules. The CISP 'Digital Dozen' was the first set of standards within the payments industry for protecting cardholder data and served as a best practices model by the G-8 conference on cyber-crime in Tokyo.

"Today, I am proud to announce an additional measure to combat identity theft and protect consumers. Our new receipt truncation policy will soon limit cardholder information on receipts to the last four digits of their accounts. The card's expiration date will be eliminated from receipts altogether. This is an added security measure for consumers that doesn't require any action by the cardholder. We are proud to be the first payments brand to announce such a move to protect cardholders' identities by restricting access to their account information on receipts.

"The first phase of this new policy goes into effect July 1, 2003 for all new terminals. I would like to add, however, that even before this policy goes into effect, many merchants have already voluntarily begun truncating receipts, thanks to groundwork that we began together several years ago.

"Receipt truncation is good news for consumers, and bad news for identity thieves. Identity thieves thrive on discarded receipts and documents containing consumers' information such as payment account numbers, addresses, Social Security numbers, and more. Visa's new policy will protect consumers by limiting the information these thieves can access.

"Visa's new receipt truncation measure builds upon our other security measures I mentioned, zero liability cardholder protection, Verified by Visa, neural networks and the Cardholder Information Security Program.

"Our receipt truncation policy is the latest initiative in Visa's broader identity theft consumer protection effort. I can't go into the details at the moment, but we will be announcing a series of additional steps to combat identity theft and offer tools to consumers.

Page 18

Visa USA Announces Account Truncation Initiative to Protect Consumers from ID Theft; Visa CEO Announces New Initiative at Press Conference With Sen. Dianne Feinstein PR Newswire March 6, 2003 Thursday

"Visa is focused on maintaining the trust we have earned through our security leadership. Because there is no silver bullet to eliminate identity theft, we are constantly adding new layers of security to protect cardholders. As a result of these, and many other security measures, fraud within the Visa system has fallen to an all-time low of just 7 cents per \$100 transacted.

"Visa USA is pleased to be working with Senator Feinstein, and the other senators here today in the fight to protect consumers from identity theft. We look forward to continuing our joint efforts; after all, we share the same goals."

About Visa

Visa is the world's leading payment brand and largest consumer payment system, enabling banks to provide their consumer and merchant customers with a wide variety of payment alternatives. Nearly 21,000 financial institutions worldwide rely on Visa's processing system, VisaNet, to facilitate \$2.4 trillion in annual transaction volume with virtually 100 percent reliability. Consumers in more than 150 countries carry more than one billion Visa-branded cards, accepted at 30 million locations around the world. Within the United States, nearly 14,000 financial institutions issue more than 385 million Visa cards, accounting for \$970 billion in annual transaction volume. Visa offers a trusted, reliable and convenient way to access and mobilize financial resources -- anytime, anywhere, anyway. For more information about Visa, please visit <http://www.visa.com>.

SOURCE Visa USA

CONTACT: Adam Bromberg, +1-703-683-5004, ext. 102, for Visa USA

URL: <http://www.prnewswire.com>

LOAD-DATE: March 7, 2003